Hon. James L. Robart

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. VOLODYMYR KVASHUK, Defendant.	NO. CR19-143JLR GOVERNMENT'S SENTENCING MEMORANDUM

The United States of America, by and through Brian T. Moran, United States Attorney for the Western District of Washington, and Michael Dion and Siddharth Velamoor, Assistant United States Attorneys, files this sentencing memorandum.

Defendant Volodymyr Kvashuk was convicted after trial of wire fraud, aggravated identity theft, and other offenses. The United States recommends a total sentence of 120 months.

I. FACTUAL BACKGROUND

The following paragraphs summarize the evidence at trial.

Kvashuk's Role at Microsoft

Kvashuk is a former software engineer at Microsoft Corporation ("Microsoft").

Kvashuk worked as an outside contractor to Microsoft between August 2016 and October 2017. He returned as a full-time employee in December 2017 and remained at the company until his termination in June 2018. Kvashuk's final annual salary at Microsoft was approximately $116,000.

Between August 2016 and June 2018, Kvashuk was a member of Microsoft's Universal Store Team ("UST"). UST supported the Microsoft online store, an internet-accessible Microsoft digital marketplace on which people can buy physical items (e.g., laptops, video-game consoles, tablets, and phones) and digital products (e.g., software). UST wrote the programming code that operates the online store, and tested that code to ensure that it worked as intended.

To simulate the customer experience on the Microsoft online store, UST members took some of the steps that an ordinary customer would take. For instance, UST members set up accounts on the Microsoft online store, browsed the online store's offerings, and added items to digital shopping carts. UST members registered these "test accounts" using digital credentials—namely, email addresses, usernames, and passwords—which were created specifically for the purpose of testing. Microsoft also gave UST members artificial payment devices (i.e., phony credit cards), named "Test in Production" ("TIP") cards, that could be used to "make payment" for products purchased using test accounts. The testimony at trial showed that Kvashuk had access to the usernames and passwords for other employees' test accounts.

Kvashuk's Theft From Microsoft

Kvashuk's criminal scheme involved the use of his and other UST members' test accounts to purchase digital gift cards from the Microsoft online store. While Microsoft blocked the delivery of physical goods (e.g., laptops) purchased by test accounts, no such safeguards prevented the delivery of digital gift cards purchased by test accounts. Those digital gift cards, which Microsoft refers to as "Currency Stored Value" or "CSV," are a form of digital currency that anybody can use in order to purchase items on the Microsoft online store. To redeem the value of a digital gift card, a purchaser must use a 25-digit "5x5" code that Microsoft generates at the time the digital gift card is purchased.

Kvashuk used test accounts to obtain over $10 million in CSV between 2017 and 2018. Two of these test accounts were assigned to other Microsoft employees, namely "Z.J." and "A.C." Kvashuk used a small amount of that CSV to purchase physical products from the Microsoft online store, and re-sold the vast majority of the CSV on an online marketplace called Paxful.

In July 2019, law-enforcement agents searched Kvashuk's lakefront home in Renton. Kvashuk purchased the home using approximately $1.675 million in criminal proceeds in April 2018. Inside the home, agents found numerous records that incriminated Kvashuk, such as: (1) an electronic document that contained Kvashuk's working notes during the criminal scheme, including the email addresses and other log-in information for the compromised test accounts; (2) screenshots of 5x5 codes, which had been purchased using the compromised test accounts and displayed on Kvashuk's computer monitor at the time of purchase; (3) files that that tracked numerous 5x5 codes that had been purchased using the compromised test accounts; and (4) proof that Kvashuk had installed tools on his digital devices that anonymized aspects of his internet activity.

Agents also found the script for a computer program that Kvashuk had created called "purchasetest." The "purchasetest" program automated the process of stealing CSV from test accounts, and spared Kvashuk from the time-consuming steps of logging into various accounts, placing orders, receiving confirmations, and tracking 5x5 codes. The "purchasetest" program was critical to the fraud because it allowed Kvashuk to steal a massive amount of CSV in a relatively short time. For example, Kvashuk used the purchasetest program to steal over $1 million in CSV via the "zabeerj2" account in a little over a day.

Kvashuk's Knowledge Of His Wrongdoing

The evidence showed that Kvashuk knew he was committing crimes and went to great lengths to conceal them. Of the approximately $10 million in CSV that he stole from Microsoft, Kvashuk purchased less than 1% using the vokvas account assigned to him. Rather, Kvashuk purchased the vast majority of CSV using other UST members' test accounts in order to frustrate Microsoft's ability to tie him to the thefts. Kvashuk lied to Microsoft investigators at two separate recorded interviews. Kvashuk used the Private Internet Access ("PIA) internet-anonymization software to erase his digital trail. After selling stolen CSV on Paxful.com, Kvashuk typically took the bitcoin he earned and ran it through "mixers" before depositing it in his Coinbase account.

Kvashuk also filed false tax returns that concealed the income from his criminal scheme. As IRS Revenue Agent Paul Shipley testified at trial, Kvashuk underreported his income for both the 2017 tax year and the 2018 tax year. More specifically: (a) Kvashuk reported $114,103 in income for 2017, even though his actual income, accounting for unreported CSV, was $1,085,237; and (b) Kvashuk reported $83,895 in income for 2018, even though his actual income, accounting for unreported CSV, was $7,469,625.

II. PROCEDURAL HISTORY

Kvashuk was arrested on July 16, 2019, and has been in custody since. The jury returned its verdicts on February 25, 2020, and convicted Kvashuk of the following charges: access device fraud (Count 1), unauthorized access to a protected computer (Count 2), mail fraud (Count 3), wire fraud (Counts 4-8), making and subscribing to false tax returns (Counts 9-10), money laundering (Counts 11-16), and aggravated identity theft (Counts 17-18).

II. PENALTIES AND SENTENCING GUIDELINES CALCULATIONS

The Probation Office calculates the Sentencing Guidelines as follows:

Count Group 1 (Access Device Fraud, Mail Fraud, Wire Fraud, Money Laundering)

Base offense level	7 (§ 2B1.1(a)(1))
Loss over $9.5 million	20 (§ 2B1.1(b)(1)(K))
Unauthorized access device	2 (§ 2B1.1(b)(11))
Sophisticated means	2 (§ 2B1.1(b)(10)(C))
Total	31

Count Group 2 (False Tax Return)	
Base offense level	20 (§§ 2T1.1(a)(1), 2S1.3(c)(1))
Income from crime	2
Total	22

As discussed below, the United States urges the Court to apply two additional enhancements: use of a special skill (to Group 1) and obstruction of justice (to Groups 1 and 2). This would result in a total offense level of 35, an advisory Guidelines range of 168-210 months, and – with the 24-month consecutive sentence for Aggravated Identity Theft factored in – an effective sentencing range of 192-234 months.

Use of a Special Skill

Kvashuk's use of his computer programming skills to commit the fraud triggers a two-point enhancement for use of a "special skill" under Section 3B1.3 of the Guidelines. The provision applies if the defendant: (a) "used a special skill;" and (b) used the skill "in a manner that significantly facilitated the commission or concealment of the offense." U.S.S.G. § 3B1.3. The skill must be "pre-existing" and "legitimate." *United States v. Green*, 962 F.2d 938, 944 (9th Cir. 1992).

Kvashuk's computer programming is a "special skill." The Guidelines defines "special skill" as "a skill not possessed by members of the general public and usually requiring substantial education, training or licensing. Examples would include pilots, lawyers, doctors, accountants, chemists, and demolition experts." U.S.S.G. § 3B1.3

comment. (applic. note 2). "Although the Guidelines provide that special skills "usually" require substantial education, training or licensing . . . such education, training or licensing is not an absolute prerequisite for a special skill adjustment." *Green*, 962 F.2d at 507. Accordingly, courts have found that a variety of skills qualify as "special skills," including ability to safely drive an 18-wheeler and advanced radio operator." *Id.*

The Ninth Circuit has held that "sophisticated computer skills" may qualify as "special skills." *United States v. Petersen*, 98 F.3d 502, 506 (9th Cir. 1996). Kvashuk's resume shows that he is a trained and highly experienced software engineer. Exhibit A, Trial Exhibit 212. Kvashuk earned a master's degree, studying (among other things) "web & object programming" and "database management." Kvashuk worked in several programming jobs, and was Chief Technology Officer of a start-up. *Id.* Kvashuk's advanced programming talent is a "skill not possessed by members of the general public[.]" U.S.S.G. § 3B1.3 comment.

Kvashuk's programming experience "significantly facilitated" his fraud. U.S.S.G. § 3B1.3 (emphasis added). The Ninth Circuit has explained that the enhancement applies "if the special skill made it *significantly easier* for the defendant to commit or conceal the crime." *United States v. Petersen*, 98 F.3d 502, 506 (9th Cir. 1996) (emphasis added, citation and internal quotation marks omitted). Kvashuk's computer skills were critical to the fraud, as they enabled him to write the "purchasetest" software program that automated his theft of CSV.

The evidence showed that, in order to manually obtain CSV from a test account, Kvashuk would have to log into the account, select CSV to purchase from the Microsoft online store, execute the order, receive a confirmation email, and then record and track the 5x5 codes. At some point, Kvashuk created "purchasetest," which automated the process and allowed him to commit fraud on a massive scale. For example, Kvashuk used "purchasetest" to obtain over $1.3 million in CSV via the "zabeerj2" test account in a little more than a day. Accordingly, the "special skill" enhancement applies.

Obstruction of Justice

Section 3C1.2 provides for a two-level enhancement if the defendant "willfully obstructed or impeded, or attempted to obstruct or impede, the administration of justice with respect to the investigation, prosecution, or sentencing of the instant offense of conviction," and "the obstructive conduct related to . . . the defendant's offense of conviction and any relevant conduct[.]" Application Note 4 lists committing "perjury" as an example of covered conduct.

Kvashuk committed perjury during the trial. He denied that he intended to defraud Microsoft, and claimed that the fraudulent scheme was actually part of a secret project intended to benefit Microsoft. Kvashuk admitted to lying to his tax preparers and failing to report income on his tax returns, but claimed that he did not intend to defraud the IRS. This testimony was outlandish and was rejected by the jury. The two-level obstruction enhancement applies.

III. SENTENCING RECOMMENDATION

This is a case of pure greed. Volodymyr Kvashuk had a life that many people would envy: at age 24, he had a master's degree and was making $116,000 a year in his dream job at Microsoft. Nevertheless, he decided to embark on a massive fraud scheme and steal millions from his employer. When Microsoft shut down two of the test accounts Kvashuk was using, he switched to a third account and used his "purchasetest" program to steal another $1.3 million in a final frenzy.

Kvashuk used the proceeds to live the life of a millionaire, driving a $160,000 car and living in a $1.6 million waterfront home. Kvashuk's scheme involved lies and deception at every step. He put his colleagues in the line of fire by using their test accounts to steal CSV. Rather than taking responsibility for his crimes, he testified and told a serious of outrageous lies. There is no sign that Kvashuk feels any remorse or regret.

Although Kvashuk's crimes are serious, he is young and has no criminal history. Furthermore, Kvashuk will almost certainly be deported. Accordingly, the United States recommends a below-Guidelines sentence of 96 months of imprisonment for Counts 1 through 16. In conjunction with the mandatory 24 months of imprisonment for Counts 17 and 18, the total recommend sentence is 120 months and three years of supervision.

Kvashuk is also responsible for $8,344,586.31 in restitution. This figure is the total value of CSV that was actually redeemed by the third parties who purchased stolen gift cards from Microsoft. Docket no. 1, Complaint, para. 14. The restitution amount is less than the loss amount $10 million because Microsoft was able to block the redemption of roughly $1.8 million in CSV.

DATED this 2nd day of November, 2020.

Respectfully submitted,

BRIAN T. MORAN
United States Attorney

/s/ Michael Dion
MICHAEL DION
Assistant United States Attorney
700 Stewart Street, Suite 5220
Seattle, WA 98101-1271
Telephone: (206) 553-7729
Fax: (206) 553-0882
E-mail: Michael.Dion@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on November 2, 2020, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the attorney(s) of record for the defendant.

/s/ Elizabeth Gan
ELIZABETH GAN
Legal Assistant
United States Attorney's Office
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
Phone: (206) 553-4370
FAX: (206) 553-0882
E-mail: Elizabeth.Gan@usdoj.gov